文章编号:1001 - 9081(2007)05 - 1257 - 03

嵌入式无线局网安全检测方案的研究与实现

吕家亮,陈 静,武 鲁
(山东省计算中心 山东省计算机网络重点实验室,山东 济南 250014)
(lvjl@keylab.net)

摘 要:研究了无线局域网数据包捕获技术、无线帧解码技术及无线局域网安全检测方法等技术。采用了无线网卡监听技术,对 WLAN 中传输的数据帧进行实时监控。通过对数据帧的分析,提出了网络性能测试和 802.1x 认证的检测方法,并用直观的方式显示无线网络的运行状况。在此基础上,提出了一个完整的无线局域网(WLAN)安全检测方案,并详细介绍了嵌入式 WLAN 安全检测系统的实现。

关键词:无线局域网;安全检测;监听;AP;802.1x
中图分类号: TP393.08 **文献标识码**:A

Research and realization of an embedded WLAN security detection project

Lü Jia-liang, CHEN Jing, WU Lu
(*Center of Shandong Computer Science, Key Laboratory for Computer Network of Shangdong, Jinan Shandong* 250014, *China*)

Abstract: Wireless packets capturing and the technology of decoding frame and security detection method were analyzed. The technique of wireless net card monitoring mode was adopted to supervise the wireless frame. From the analysis of data frame, detecting methods of performance testing and 802.1x authentication were brought forward, and the network status was displayed in the intuitionistic way. On this basis, a WLAN security detection plan was presented and the design of WLAN security detection system was described in detail.

Key words: WLAN; security detecting; monitor mode; AP; 802.1x

0 引言

无线局域网(WLAN)是无线通信技术和计算机网络的结合体。它利用无线技术在空中传输数据、话音和视频信号,把用户从有线网络中解放了出来,使他们可以随时随地获取信息,提高了员工的办公效率。又由于无线局域网拥有可移动性、布线容易、组网灵活及成本优势等特点,促进了无线时代的来临,在各行业的广泛应用取得了令人注目的成果,展示了极为广阔的前景,它将为我们创造崭新的生活和工作风尚。目前,已经有越来越多的企业认识到无线局域网的优势,并且开始借助无线技术来解决问题。

但是当我们为无线局域网的应用前景惊叹时,无线局域网应用过程中也出现了一些问题,如:接入点的覆盖面积难以确定,传输数据的安全性难以保证,网络不易于管理,信道容易受到干扰等。因此,要想实时的对无线局域网的安全状况或性能状况进行测试,一种理想的设计方案就是开发嵌入式便携设备,通过直观、智能先进的操作界面解决无线局域网在规划、设计、安装、维护及管理等各个阶段所遇到的问题。

目前在无线局域网的嵌入式设备研究方面,国外主要有美国 Fluke 网络公司推出的无线通和艾尔麦公司推出的无线局域网测试仪,这两种测试仪的功能相似,能够完成大部分的无线局域网测试任务,但是他们的测试功能都是基于 PDA,没有自己开发的硬件系统;而在国内对于无线局域网的研究主要集中网络无线扩展、漫游、无线安全等关键基础技术的研究,没有涉及无线局域网测试系统的应用研究。本文正是在这一基础上开发设计了一套嵌入式 WLAN 检测系统,以期能够解决无线局域网的安全检测。

1 系统方案设计

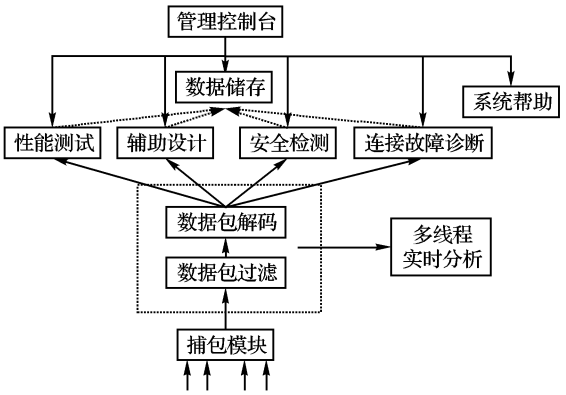

图 1 WLAN 安全检测系统架构图

无线局域网安全检测系统的软件主要包括了管理控制界面、安全检测分析模块、无线捕包模块。其中安全检测分析模块是整个软件的核心部分。整个系统采用 Linux 操作系统作为开发平台,采用目前比较流行的 qte/qtopia 开发环境来实现友好的人机交互界面,此环境支持中文图形界面、多窗口同时显示,安全稳定。安全检测分析包括网络的性能测试、网络辅助设计、协议分析、安全分析、连接故障诊断等,每个模块独

收稿日期:2006 - 10 - 31;**修订日期**:2007 - 01 - 26 **基金项目**:山东省自然科学基金资助项目(Q2005G02)
作者简介:吕家亮(1982 -),男,山东东营人,硕士研究生,主要研究方向:网络、网络安全; 陈静(1978 -),女,山东济南人,副研究员,硕士研究生,主要研究方向:光学工程、无线网络测试; 武鲁(1982—),男,山东菏泽人,硕士研究生.

立功能检测,通过网络适配器与所要测试的网络连接,依据内部的数据处理规则与网络上的数据进行交互,最后将经过处理的测试结果通过下层的 Qtopia 图形用户界面直观的显示给最终用户。软件的总体架构如图 1 所示。

2 功能模块介绍

嵌入式无线局域网安全检测系统是一个对无线局域网进行全方位、综合的、多层面的测试系统。主要包括智能数据采集分析、无线局域网的性能测试、安全检测、网络辅助设计和连接故障诊断等五大功能。

2.1 智能数据采集分析

数据采集是整个系统的基础。无线网卡有两种工作模式:一是正常模式;一种是射频监听模式[2]。在正常模式下,网卡只接收帧的目的地址与本网卡的 MAC 地址相同的数据帧和广播帧,而如果把网卡设置为射频监听模式,便能够接收到局域网内所有的数据帧。因此我们采用网卡的监听模式在后台捕获无线局域网 802.11b/g 性能数据。根据数据帧不同性能参数自动提取特征数据,提供给上层应用程序进行 WLAN 实时测试,以识别和跟踪无线设备及其不同的特征,监测和分析 WLAN 的健康情况;并对特征数据进行分类存储,回放测试过程记录的相关数据,供再次分析使用。

2.2 无线局域网性能测试

为了提高无线网络设备的利用率,要采用先进的技术手段及合理的测试方法,实现无线局域网的科学规划、优化和合理设计。性能测试主要测试网络的信号状况及整体状态。对网络上所有的 SSID(服务组标志符),AP 以及站点(授权或非授权)进行分类,给安装人员提供 WLAN 站点图。允许对接入点进行详细的探查,来评估信号质量以及不同设置选项。测试通道信号及噪声强度,帮助识别和隔离来自不明接入点和其他潜在信源的联合信道干扰,防止可能的冲突和性能问题。由于无线局域网的网络故障的原因有很多,但大多无线网络故障都可以通过协议分析进行检测,所以网络维护中协议分析是必不可少的手段之一,甚至一些无线网络连通性的故障原因也可以通过协议分析进行诊断。由于无线局域网在协议下两层与有线网的帧格式不同,因此该模块主要对 802.11b协议和 802.11g 协议进行分析研究,找出其中的异同点,有利于对 802.11b 和 802.11g 的混合网络进行测试。对捕获的管理帧、控制帧、数据帧进行解码,分析网络故障的原因。

2.3 安全信息检测

目前,无线局域网应用过程中出现了比较多的安全问题。早期的 802.11 标准,一些已经内置的安全功能所提供的安全保护并没得到执行,这多数是由于不具备网络专业知识的非技术人员安装 Wi-Fi 硬件造成的,这就为企业网络遭受安全攻击打开了方便之门。故对 WLAN 应该进行全面的安全测试,发现潜在的安全问题。主要包括:检测未经授权就进入网络的设备,探测典型的无线拒绝服务攻击(侵者通过大量占用 WLAN 信道或使用 AP 关联表数据溢出)的方法造成拒绝网络访问故障。对伪装 AP 进行探测,并搜寻未被 802.1x 保护的 WLAN 设备。

2.4 连接故障诊断

没有智能的工具,要进行连接问题故障诊断所耗费专业人员的精力和时间是不可想象的,为了帮助排除相关的问题,我们在内部集成了一套智能的连接诊断工具,来识别网络连接时不匹配故障和认证、连接等问题。主要是识别 SSID,WEP 码,传输速率或 RF 信道不匹配故障,帮助隔离与特定接入点间的连接问题,包括 Ping,路由追踪,Whois 和 DNS 查询等。

3 关键技术分析

3.1 libpcap 捕包原理和方法

Libpcap 是由洛仑兹伯克利国家实验室编写的 Linux 系统下的捕包函数库,通过调用 Libpcap 中接口函数可以直接与内核驱动程序交互,实现网络信息的监听,大多数网络监控软件都可以以它为基础。Libpcap 可以在绝大多数类 UNIX 平台下工作,其重点是 Linux 的底层包捕获机制和过滤器设置方式。Libpcap 应用程序从形式上看很简单,其捕包过程大体可以分为四个步骤,分别是建立监听会话,设置过滤规则,捕获数据包和调用回调函数。

3.2 套接字捕包原理和方法

套接字是 TCP/IP 和应用程序之间的接口(API),应用程序在网络上传输、接收信息都通过 Socket 接口来实现,在应用开发中就像使用文件句柄一样,可以对 Socket 句柄进行读、写操作。Linux 下的 socket 编程比较简单,主要通过生成套接字、与本地地址绑定、读取数据等几个步骤组成。

通过对以上两种捕包方式的研究,我们发现两种方法各有利弊,利用 libpcap 库进行捕包可以方便的设置过滤规则,能够有效的对数据包进行过滤;但是它的运行效率要低于 Linux 内核提供的 socket 捕包机制,因为 libpacp 毕竟是第三方开发的捕包函数库,它不同于 Linux 内核直接提供的捕包机制。由于嵌入式系统的运行速度和资源具有有限性,对于实时性要求比较高的捕包程序来说,实时性是第一位的,因此在系统的开发过程中,我们采用了两套方案。即在 pc 机上开发时,我们采用了 libpcap 捕包方式,在嵌入式设备上采用了 socket 捕包方式,确保了程序的合理性。

3.3 无线帧解码技术

IEEE 802.11g 和 802.11b 协议的区别主要是表现在物理层和 MAC 子层上。因为要对捕获的数据包进行解码区分,而网卡所能捕获到的最原始的数据包是从 MAC 层开始的,所以有必要对两种协议的 MAC 子层进行研究和分析。而对物理层的区分在此就不再赘述了。

(1) 控制帧:两种协议在控制帧的格式方面基本上是一样的,唯一的区别是在 CTS(请求发送帧)帧的 Duration 字段的值的计算方法不同,并不影响系统的协议分析系统。

(2) 管理帧:两种协议在 MAC 帧上的最主要的区别就是在管理帧格式的定义上。首先,由于物理层的调频方式不同,导致了在管理帧的帧体中 AP 的信道数是由不同的调频方式产生的。其次,在支持速率(Supported Rates)字段,802.11b 支持的最大速率为 11Mbps,而 802.11g 支持的最大速率为 54Mbps,支持速率的个数不同。再次,在 802.11g 的帧体定义中,增加了 ERP Information 字段和扩展支持速率(Extended Supported Rates)字段。

(3) 数据帧:由于数据帧涉及到上层协议的定义,所以两种协议在数据帧的格式定义方面并没有区别。对两种不同协议的数据帧进行解码时,可以按照统一的标准进行。

对无线局域网中的帧进行解码是分析网络性能的首要步骤,对无线帧进行解码涉及到管理帧、控制帧和数据帧,因为管理帧和控制帧只涉及无线局域网络的 MAC 层,而没有网络

层及高层数据,其 MAC 帧头中各字段及帧体部分在 802.11 协议中都有详细定义,可以直接进行解码

3.4　非法设备检测

所谓非法设备检测是指检测网络中未被授权的设备(AP 和移动终端)和伪装接入点的过程。传统的检测方法主要有两种:一种是通过无线局域网控制器的形式对接入网络的设备进行认证检测,目前 cisco 公司已经有成熟的产品,但是这种设备价格比较昂贵,对于小型或中型的无线局域网用户来说是很不经济的。另一种是通过在网络中布置一定数量探测器,然后通过他们向服务器发送捕获的数据,由服务器的管理控制程序对数据进行分析,把检测的结果通过浏览器的方式展示给网络管理员。通过对以上两种检测方式的分析,我们发现这两种方案比较适合大型的无线局域网用户,并且只支持几种硬件设备。因此对于目前比较流行的企业、校园等小型局域网,不具有很强的适用性。

为了保护中小型局域网的安全,本文提出了一种基检测、分析、显示于一体的移动解决方案。该方案首先要建立一个合法设备的 MAC 地址列表,俗称白名单,通过嵌入式设备上的无线网卡监听网络,捕获网络中通信数据包,然后采用多线程技术将捕获的数据进行实时分析,将分析的结果和白名单中的 MAC 地址进行逐一比较,从而发现非法的设备和介入点。并最终在友好的图形界面中显示出来。这样用户只要手持嵌入式设备在布网的空间中移动即可迅速的检测到局域网内的非法设备,具有很好的灵活性和实用性。

3.5　802.1x 认证检测的实现

随着网络建设规模的迅速扩大,网络上原有的 WEP 认证系统已经不能很好的适应用户数量急剧增加的要求,如何通过端口认证来防止其他公司的计算机接入本公司内部网就成为一项非常现实的问题,IEEE 802.1x 协议就是基于这一需求而出现的一种基于端口的网络接入控制技术。就是认证用户从网络边界接入网络,网络管理员也可以确保没有认证的用户无法访问网络,让所有用户的认证都可以集中在一个验证服务器上完成。

本文在深入研究了 IEEE802.1x 协议的体系结构、认证机制等关键技术的基础上,提出了一种跟踪 802.1x 认证过程的方法,通过这种方法能够快速查找出认证失败的原因并搜寻未被 802.1x 保护的设备,从而能够方便快速的对无线局域网中的设备进行安全设置。

802.1x 认证中客户端、认证端和认证服务器之间的认证过程在此不在赘述。如果认证服务器认可这客户端,即认证通过,那么认证服务器会通知认证端将转换这客户端的端口到授权状态并转发其他的通信,否则保持受控端口的关闭状态。认证端 PAE(Port Access Entity)控制其可控端口的操作状态,但他不会干涉客户端 PAE 和认证服务器之间的认证数据交换。也就是说即使客户端没有通过认证,客户端和认证服务器之间传输的认证帧也是可以通过认证端进行转发的。认证端 PAE 的主要功能是用来中转客户端和认证服务器之间的 EAP 帧,它把来自客户端 PAE(认证服务器)的 EAP 帧重新打包,生成认证服务器(客户端 PAE)可以识别的帧格式后传输给认证服务器(客户端 PAE)。在无线局域网中,认证端即我们常用的 AP,因此客户端和认证端之间传输的认证帧是能够捕获到的。通过分析 EAPOL 帧和 EAP 消息帧的格式,我们发现,EAP 的消息帧中有一个 code 字段,如果 code 的值等于 3,表明认证成功,即该设备受到了 802.1x 的保护;如果 code 的值等于 4,表明认证失败,即该设备没有受到 802.1x 的保护。因此我们可以跟踪 802.1x 的认证过程,捕获认证过程中的认证帧,分析认证失败的原因,从而搜寻出未被802.1x 保护的设备。

4　系统的实现

系统一启动便会直接进入主界面,共包含 7 个主模块分别是:网络配置、性能测试、安全检测、辅助设计、连接故障诊断、网络报告和帮助系统。模块之间的工作流程如下:用户通过点击控制面板上的图标来启动上层的功能模块,进入相应的功能页面(如图 2 和图 3),功能模块启动后,便会启动一个辅助线程[6]开始探测网络。功能模块在探测网络的同时,将所得结果返回给主线程,主线程通过窗口上的显示控件将探测结果返回给用户。当用户点击配置页面上的退出按钮或关闭相应模块的图形界面时,功能模块关闭消息队列、销毁主窗口后系统退出。

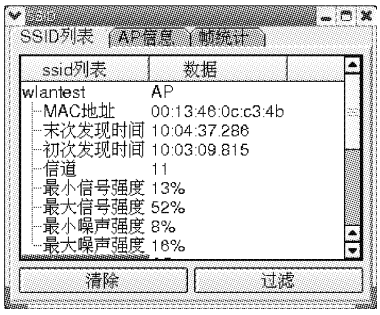

图 2　SSID 列表显示界面

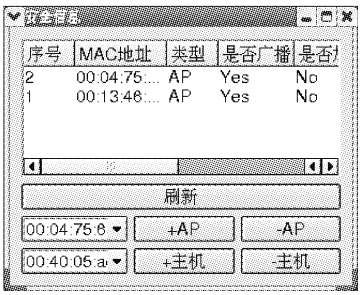

图 3　安全信息检测界面

5　结语

在 WLAN 飞速发展的今天,其稳定性和安全性已经成为人们非常关心的问题。本文针对无线网络移动性的特点,提出了一种理想的安全检测方案,并在此基础上开发了嵌入式无线局域网安全检测系统,从而进一步验证了检测方案的可行性。而且具有良好的扩展性和可移植性。但是由于捕包分析对系统的实时性要求非常高,所以在安全检测系统的性能方面我们还应该做进一步的研究。

参考文献:

[1]　刘乃安. 无线局域网(WLAN)——原理、技术与应用[M]. 西安:西安电子科技大学出版社,2004.

[2]　谭思亮. 网络与监听[M]. 北京:人民邮电出版社,2002.

[3]　GEIER J. 无线局域网[M]. 王群,李馥娟,叶清扬,译. 北京:人民邮电出版社,2001.

[4]　张丰翼,刘晓寒,马文平,等. 无线局域网安全的关键问题[J]. 信息安全与通信保密,2004,(5).

[5]　严照楼,潘爱民. 无线局域网的安全性研究[J]. 计算机工程与应用,2004,(5).

[6]　张威. 网络编程教程[M]. 北京:希望电子出版社,2002.